

E S T

Cisco VPN Client Installation and Configuration for Windows XP and 2000

4 June 2004

This document contains information EXEMPT FROM MANDATORY DISCLOSURE under the FOIA. Exemption number 5 applies (internal advice, recommendations and subjective evaluations that are reflected in records pertaining to the decision-making process of or among agencies).

Distribution Statement C

Distribution authorized to U.S. Government agencies and their contractors doing business with the Network Enterprise Technology Command NETCOM / 9th Army Signal Command. This document is available by request from: Director, NETCOM, ATTN: NETC-EST-E, 2133 Cushing Street, Fort Huachuca, AZ 85613-7070.

OPERATIONAL ENGINEERING DIRECTORATE

DEPARTMENT OF THE ARMY
NETWORK ENTERPRISE TECHNOLOGY COMMAND/9TH ASC
U.S. ENTERPRISE SYSTEMS TECHNOLOGY ACTIVITY
FORT HUACHUCA, ARIZONA, 85613-7070

DISCLAIMER

The contents of this document are not to be construed as an official Department of the Army position unless so designated by other authorized documents. The use of trade names in this document does not constitute an official endorsement or approval of the use of such commercial hardware or software. Do not cite this document for the purpose of advertisement.

CHANGES

Refer requests for all changes that affect this document to: Director, NETCOM/ESTA, ATTN: NETC-EST-E, Fort Huachuca, AZ 85613-7070.

DISPOSITION INSTRUCTIONS

Destroy this document when no longer needed. Do not return it to the organization. Safeguard and destroy this document with consideration given to its classification or distribution statement requirements.

MICHAEL GRAFTON		GLEN GRIFFIN
Electronics Engineer		Senior Engineer
ROBERTO SUAREZ		PETER JURMAN
Chief, Enterprise Networks Division		Principal Engineer, OED
	MICHAEL D. BOMBA	_

Director, OED

EXECUTIVE SUMMARY

The following	document provid	es instructions	s on how to	install and	configure a	Cisco	VPN
Client on Wind	lows XP and 200	0.					

This page intentionally left blank

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

1.0	INTRODUCTION	1
	INSTALLATION OF VPN CLIENT SOFTWARE	
3.0	CONFIGURATION OF VPN CLIENT	12
3.1	CONFIGURATION OF VPN CLIENT USING CAC AUTHENTICATION	12
3.2	CONFIGURATION OF VPN CLIENT USING GROUP AUTHENTICATION	20

This page is intentionally left blank.

FOR OFFICIAL USE ONLY

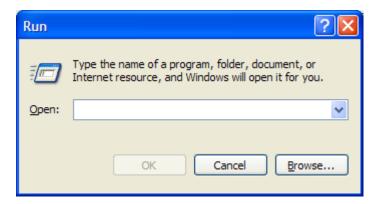
1.0 INTRODUCTION

The following document provides instructions on how to install and configure a Cisco VPN Client on Windows XP and 2000. The screenshots shown in this document are from Windows XP. Some of the screenshots in this document will vary slightly when installing on Windows 2000, but are essentially the same and noted where applicable. Also, if another version of Cisco VPN Client is installed the screens shown might vary.

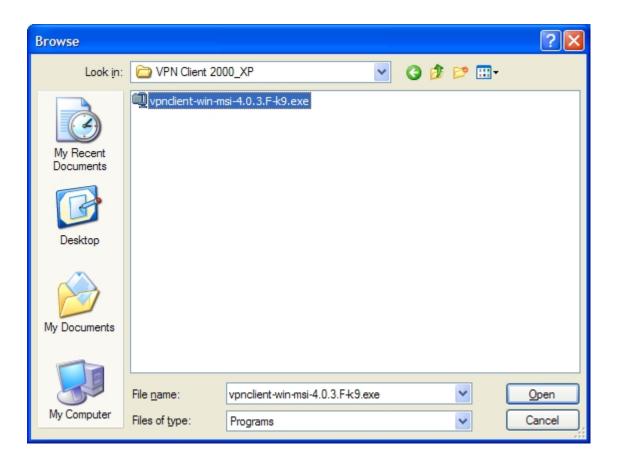
2.0 INSTALLATION OF VPN CLIENT SOFTWARE

The person installing the VPN Client software must have administration rights on the computer.

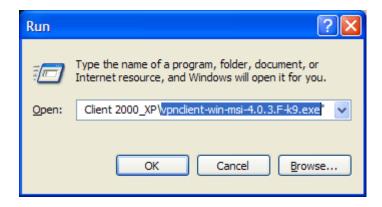
Go to the "Start" menu located in the lower left corner and select "Run" and click the "Browse..." button.



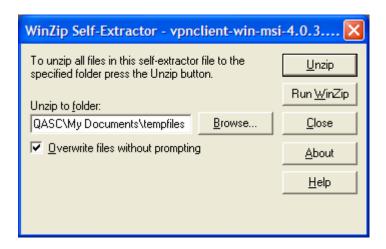
Navigate through the folders until you find the file vpnclient-win-msi-4.0.3.F-k9.exe, highlight the file and click the "Open" button.



Now click "OK". Note: Your file name and location might be different depending on the Cisco VPN Client version and where the file is located.



The ".exe" file is an executable zipped file. Go ahead and unzip the file using a program such as WinZip. Use the "Browse..." button to change where you want the files to unzip or make a note of the default unzip location. This file location only needs to be temporarily; it only needs to be used to run the Cisco VPN client setup utility.

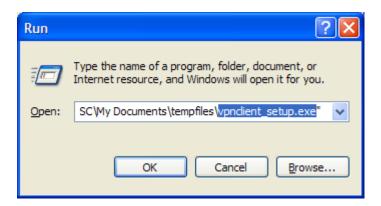


After the file is unzipped the following box appears. Note: Windows 2000 unzips 10 files and depending on the Cisco VPN Client version it might be different.



Go to the "Start" menu located in the lower left corner and select "Run", find the file "vpnclient_setup.exe" for Windows XP or "setup.exe" for Windows 2000 and click "OK". Note: Your file name and location might be different depending on the version and where you unzipped the file.

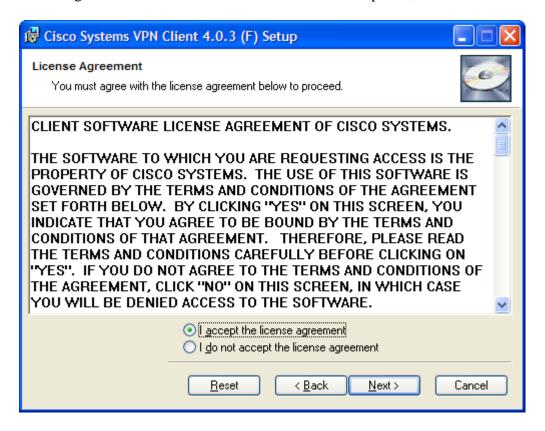
Next "Run" the Cisco VPN Client Installation Wizard located in the unzipped folder, using the same procedure as above. The file name in Windows XP is "vpnclient_setup.exe", for Windows 2000 the file name is "setup.exe". Note: Your file name and location might be different depending on the Cisco VPN Client version and where you unzipped the file.



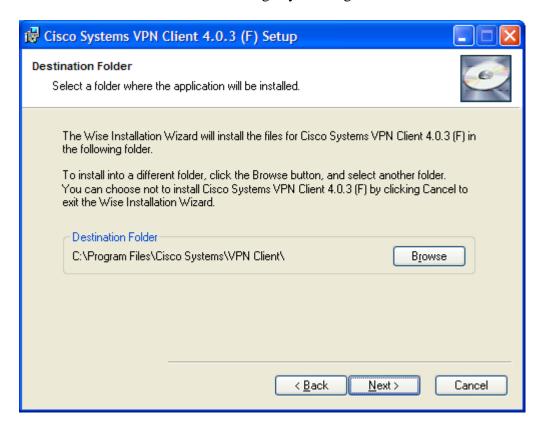
The Cisco VPN Client software Installation Wizard now appears. Continue by selecting "Next>"



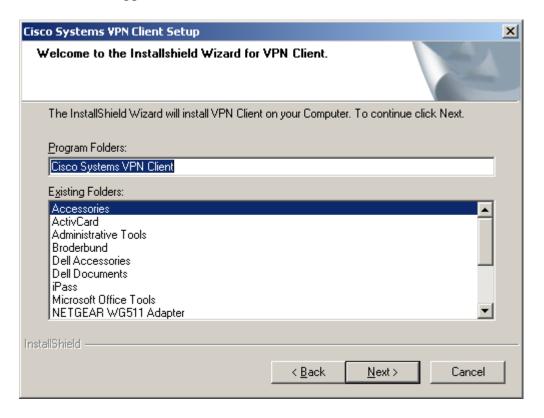
Read through the License agreement and if it's acceptable to you, mark the bullet "I accept the license agreement" and select "Next>". If it's not acceptable, abort the installation.



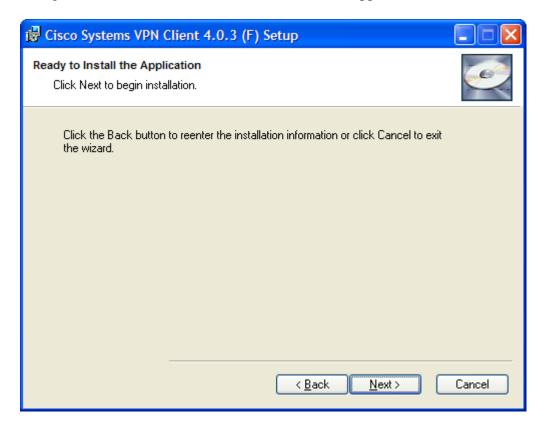
The next screen asks where the application should reside on the computer; it is highly recommended to use the default settings by clicking "Next>".



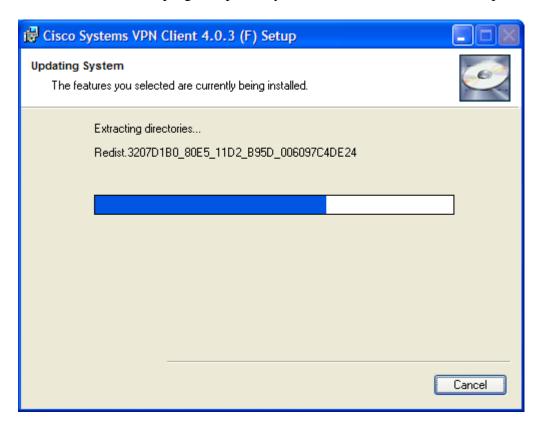
In Windows 2000 a screen appears for the placement of the Cisco VPN Client application in the program files, it is highly recommended to accept the default by clicking "Next>". Note: This screen will not appear in the Windows XP installation.



In Windows XP this screen lets you know that the application is ready to install. Click "Next>" to begin the installation. Note: This screen will not appear in the Windows 2000 installation.



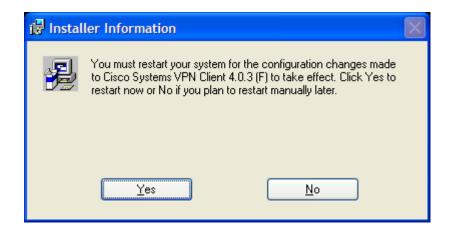
This screen shows the progress; patiently wait until the installation is complete.



After installation in Windows XP the next screen appears click "Finish". Note: In Windows 2000 this screen will not appear.



Now the computer must be restarted in order for the installation to be truly complete. Click "Yes" to immediately reboot the computer or click "No" to do it at a later time. Do not attempt to use the application until you have rebooted the computer.



FOR OFFICIAL USE ONLY

3.0 CONFIGURATION OF VPN CLIENT

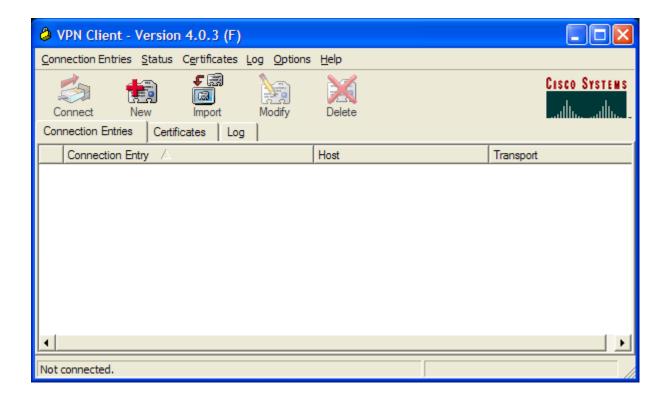
The Cisco VPN client software can use different methods for user authentication. This section describes two methods. Sub-Section 3.1 describes a configuration for the Department of Defense's (DoDs) Common Access Card (CAC). Sub-Section 3.2 describes group authentication.

For the appropriate security, both methods require the use of a second factor of user authentication, such as RADIUS.

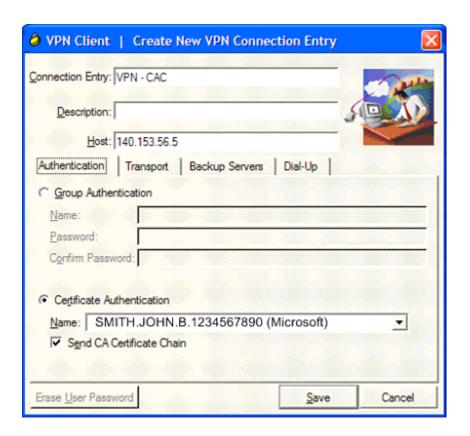
3.1 CONFIGURATION OF VPN CLIENT USING CAC AUTHENTICATION

This document assumes that the ActivCard Gold or equivalent is installed and all the required DoD and Identity certificates are registered on the computer and working correctly.

Run the Cisco VPN Client by going to the "Start" menu located in the lower left corner and select "Programs / Cisco Systems VPN Client / VPN Client". The screen below will appear.



Click on the "New" button located just below the menu options on top and fill in the entries. Note: The "Authentication" tab is opened by default when creating a new connection entry.



Connection Entry: Name the entry, this example used "VPN - CAC"

Description: Put in a description, this example left it blank

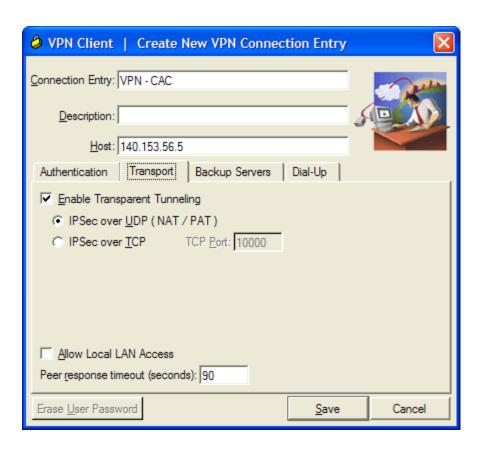
Host: The IP address of the VPN concentrator or resolvable host name, this example used "140.153.56.5"

Authentication Tab:

Mark Bullet "Certificate Authentication"

Name: Your CAC certificate, if it's not there the certificate are not installed correctly on your computer

Check Box "Send CA Certificate Chain"



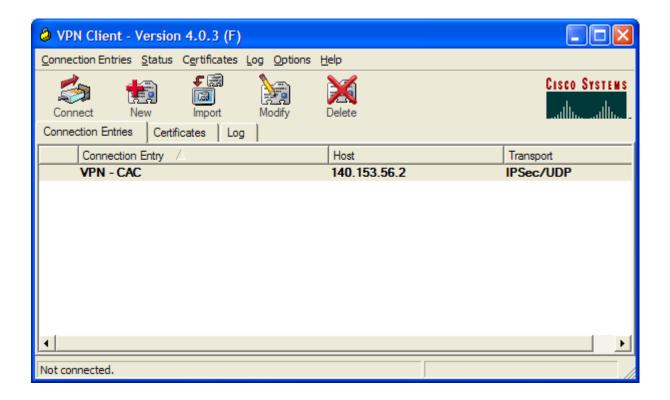
Now click on the Transport Tab:

Check "Enable Transparent Tunneling"

Mark Bullet "IPSec over <u>UDP</u> (NAT / PAT)

Click Save.

After the connection entry is saved, it appears as shown.



Next highlight the VPN - Groups Connection Entry and select the "Connect" button. The next few screens will appear if you don't have your CAC in the computer.

This screen wants you to insert your CAC.



This screen has detected and the CAC, and click "OK" to continue.



This screen prompts you for your CAC pin.

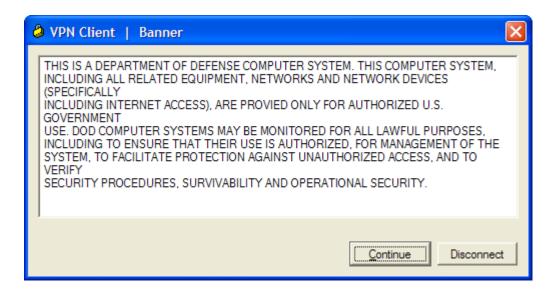


After your CAC has been entered in the computer and you have given your personal pin code, you are prompted for the second form of user authentication. This could be RADIUS authentication or another form of secure authentication.

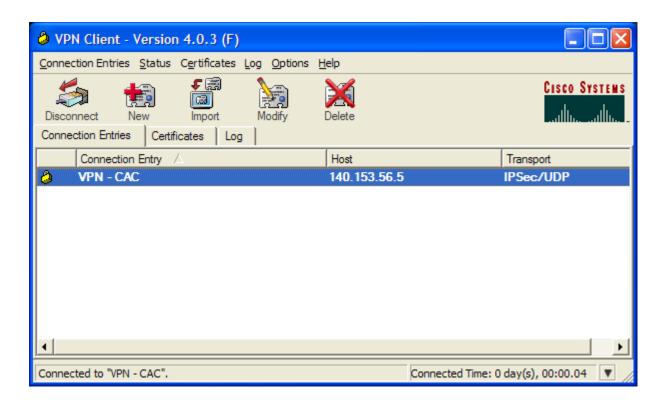


Enter your assigned Username and Password and select "OK".

After successfully being authenticated, a warning banner appears, select "Continue" and the VPN connection has now been established.

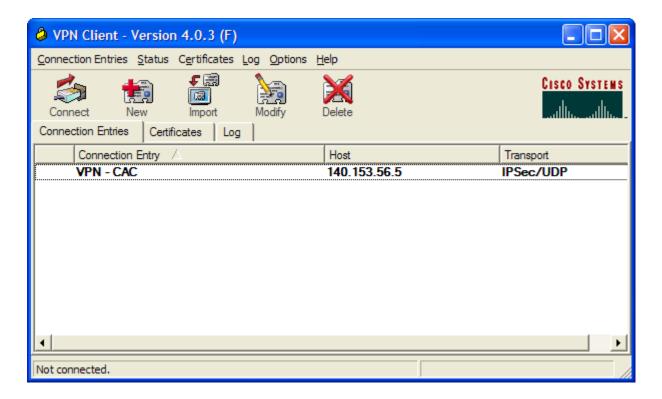


To disconnect from the VPN, bring the Cisco VPN client back up either by going to the "Start" menu located in the lower left corner and selecting "Programs / Cisco Systems VPN Client / VPN Client", or double clicking the "Pad Lock" icon located in the lower right corner. Note: This screen shows that the VPN is connected by the information provided in the lower left corner 'Connected to "VPN - CAC".



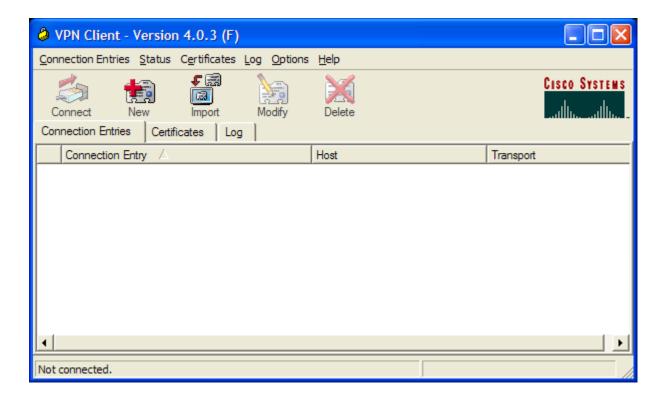
Highlight the connection entry and click the "Disconnect" button.

The VPN is now disconnected, as noted on this screen by the lower left corner information "Not connected".



3.2 CONFIGURATION OF VPN CLIENT USING GROUP AUTHENTICATION

Run the Cisco VPN Client by going to the "Start" menu located in the lower left corner and select "Programs / Cisco Systems VPN Client / VPN Client". The screen below will appear.



Click on the "New" button located just below the menu options on top and fill in the entries. Note: The "Authentication" tab is opened by default when creating a new connection entry.



Fill in the fields as shown below:

Connection Entry: Name the entry, this example used "VPN – Groups"

Description: Put in a description, this example left it blank

Host: The IP address of the VPN concentrator or resolvable host name, this example used "140.153.56.5"

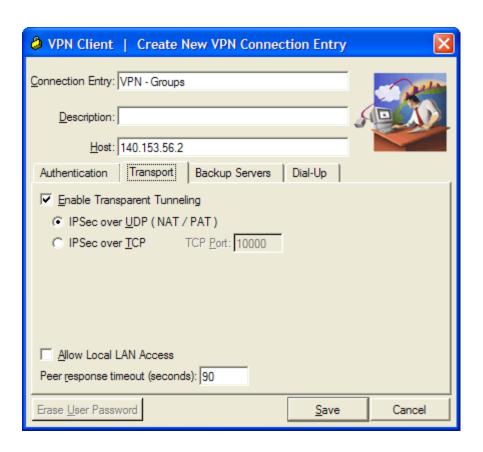
Authentication Tab:

Mark Bullet "Group Authentication"

Name: This is the group you're assigned, this example uses ipass_grp

Password: The password that is distributed securely

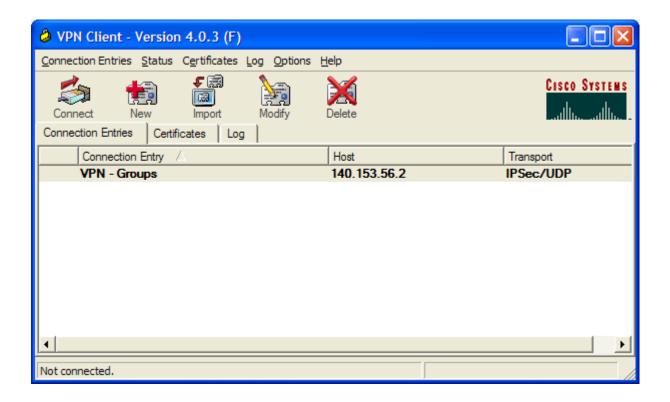
Confirm Password: The password that is distributed securely



Now click on the Transport Tab: Check the box "Enable Transparent Tunneling" Mark Bullet "IPSec over <u>UDP</u> (NAT / PAT)"

Click Save.

After the connection entry is saved, it will now appear under the "Connection Entry" tab.

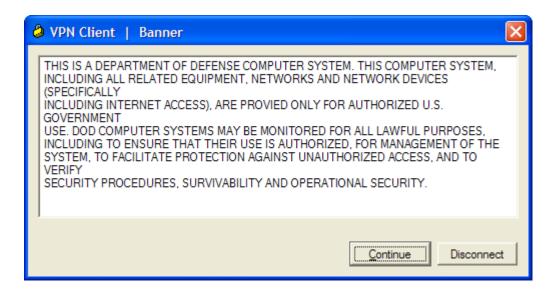


Next highlight the "VPN – Groups" connection entry and click the "Connect" button. The next screen is now requesting the second form of user authentication. This could be RADIUS authentication or some other form of secure authentication.

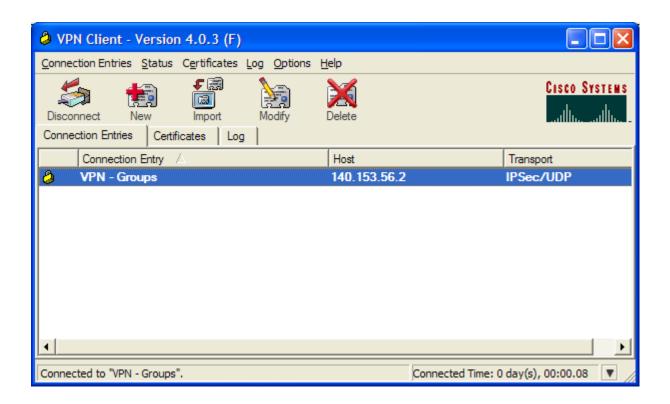


Enter your assigned Username and Password and select "OK".

After successfully being authenticated, a warning banner appears, select "Continue" and the VPN connection has now been established.



To disconnect from the VPN, bring the Cisco VPN client back up either by going to the "Start" menu located in the lower left corner and selecting "Programs / Cisco Systems VPN Client / VPN Client", or double clicking the "Pad Lock" icon located in the lower right corner. Note: This screen shows that the VPN is connected by the information provided in the lower left corner 'Connected to "VPN - Groups".



Highlight the "VPN – Groups" connection entry and click the "Disconnect" button.

The VPN is now disconnected, as noted on this screen by the lower left corner information "Not connected".

